AF/#

PATENT
Attorney Docket No. 09812.0583-00

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:

Yoshihito ISHIBASHI et al.) Group Art Unit: 2165

Application No.: 09/396,054) Examiner: Neveen ABEL JALIL

Filed: September 15, 1999) Confirmation No.: 6914

For: CONTENT MANAGEMENT METHOD, AND CONTENT STORAGE SYSTEM

Mail Stop Appeal Brief--Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

TRANSMITTAL OF APPEAL BRIEF (37 C.F.R. 41.37)

Transmitted herewith is the APPEAL BRIEF in this application with respect to the Notice of Appeal filed on October 1, 2007.

This application is on behalf of

□ Small Entity ☒ Large Entity

Pursuant to 37 C.F.R. 41.20(b)(2), the fee for filing the Appeal Brief is:

□ $255.00 (Small Entity)

☒ $510.00 (Large Entity)

TOTAL FEE DUE:

Appeal Brief Fee	$510.00
Extension Fee (if any)	$0
Total Fee Due	$510.00

☒ A check in the amount of the total fee of $510.00 is submitted herewith.

PETITION FOR EXTENSION. If any extension of time is necessary for the filing of this Appeal Brief, and such extension has not otherwise been requested, such an extension is hereby requested, and the Commissioner is authorized to charge necessary fees for such an extension to our Deposit Account No. 06-0916. A duplicate copy of this paper is enclosed for use in charging the deposit account.

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 3, 2007

By:
Reece Nienstadt
Reg. No. 52,072

PATENT
Attorney Docket No. 09812.0583-00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)
)
Yoshihito ISHIBASHI et al.) Group Art Unit: 2165
)
Application No.: 09/396,054) Examiner: Neveen ABEL JALIL
)
Filed: September 15, 1999) Confirmation No.: 6914
)
For: CONTENT MANAGEMENT)
METHOD, AND CONTENT)
STORAGE SYSTEM)

Mail Stop Appeal Brief--Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

APPEAL BRIEF UNDER BOARD RULE § 41.37

In support of the Notice of Appeal filed October 1, 2007, and further to Board Rule 41.37, Appellants present this brief and enclose herewith a check for the fee of $510.00 required under 37 C.F.R. § 1.17(c).

This Appeal responds to the May 31, 2007, final rejection of claims 1-5, 14-16, 18, 20-25, 29-34, and 38-41.

If any additional fees are required or if the enclosed payment is insufficient, Appellants request that the required fees be charged to Deposit Account No. 06-0916.

Table of Contents

I. REAL PARTY IN INTEREST

Sony Corporation is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

There are currently no other appeals or interferences, of which Appellants, Appellants' legal representative, or Assignee are aware, that will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-41 are currently pending in this application, of which claims 1-5, 14-16, 18, 20-25, 29-34, and 38-41 have been finally rejected by the Examiner. Claims 6-13, 17, 19, 26-28, and 35-37 are objected to by the Examiner as dependent upon a rejected base claim but allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The rejections of claims 1-5, 14-16, 18, 20-25, 29-34, and 38-41 are being appealed.

Further to 37 C.F.R. § 41.37(c)(1)(viii), the attached Claims Appendix contains a clean copy of the pending claims.

IV. STATUS OF AMENDMENTS

There has not been any Amendment filed after the final Office Action mailed May 31, 2007 ("final Office Action").

V. SUMMARY OF CLAIMED SUBJECT MATTER

A. Independent Claim 1

Independent claim 1 is directed to a content management method for managing content data provided to user equipment. The method includes storing a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key in the user equipment. The first storage key is stored in a key management unit. The encrypted content key and the second storage key are sent to the key management unit. At the key management unit, the encrypted content key is decrypted using the first storage key. The decrypted content key is encrypted using the second storage key. The content key, which is encrypted with the second storage key, is sent to the user equipment. At the user equipment, the encrypted content key is decrypted using the second storage key. Using the decrypted content key, the content data is decrypted.

An exemplary embodiment of this content management method is described in the Specification at, for example, pg. 14, paragraph 3 to pg. 17, paragraph 3. This embodiment is also illustrated in Figure 5 of the Specification.

B. Independent Claim 20

Independent claim 20 is directed to a content management system for managing content data. The system includes a storing means having stored therein a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key. The first storage key is stored in a key management unit. The system has a sending means for sending the encrypted content key and the second storage key to the key management unit. A first decrypting means in the key management unit is provided for decrypting the encrypted content key using the first storage key. An encrypting means is provided for encrypting the decrypted content key using the second storage key. A second decrypting means is provided for decrypting the encrypted content key using the second storage key and decrypting the content data using the decrypted content key.

An exemplary embodiment of this content management system is described in the Specification at, for example, pg. 14, paragraph 3 to pg. 17, paragraph 3. This embodiment is also illustrated in Figure 5 of the Specification.

The content management system recited in claim 20 comprises the element of "a storing means having stored therein a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key." An exemplary embodiment of this "storing means" is described in the Specification at, for example, pg. 15, paragraph 3, and pg. 16, paragraph 2. This embodiment of the "storing means" is also shown in Figure 5 of the Specification as the "external storage" at reference number 22.

The content management system recited in claim 20 further comprises the means-plus-function element of "a sending means for sending the encrypted content key and the second storage key to a key management unit." An exemplary embodiment of this "sending means" is described in the Specification at, for example, pg. 15, paragraph 3. This embodiment of the "sending means" is also shown in Figure 5 of the Specification as the "receiver" at reference number 14. An exemplary embodiment of the "key management unit" is shown in Figure 5 as the "key management center" at reference number 13.

Claim 20 further recites the means-plus-function element of "a first decrypting means, in the key management unit, for decrypting the encrypted content key using the first storage key, the first storage key being stored in the key management unit." An exemplary embodiment of this "first decrypting means" is described in the Specification at pg. 15, paragraph 3. This embodiment of the "first decrypting means" is also shown in Figure 5 of the Specification as the "key management center" at reference number 13. An exemplary embodiment of the "key management unit" is also shown in Figure 5 as the "key management center" at reference number 13.

Claim 20 also recites the means-plus-function element of "an encrypting means for encrypting the decrypted content key using the second storage key." An exemplary embodiment of this "encrypting means" is described in the Specification at, for example, pg. 15, paragraph 3. This embodiment of the "encrypting means" is also shown in Figure 5 of the Specification as the "key management center" at reference number 13.

In addition, claim 20 recites the means-plus-function element of "a second decrypting means for decrypting the encrypted content key using the second storage key and decrypting the content data using the decrypted content key." An embodiment of this "second decrypting means" is described in the Specification at, for example, pg. 16, paragraph 2. This embodiment of the "second decrypting means" is also shown in Figure 5 of the Specification as the "receiver" at reference number 14.

VI. GROUNDS OF REJECTION

A. Claims 1-5, 14-16, 18, 20-25, 29-34, and 38-41

Claims 1-5, 14-16, 18, 20-25, 29-34, and 38-41 stand rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,784,464 to Akiyama et al. ("*Akiyama et al.*") in view of U.S. Patent No. 5,319,705 to Halter et al. ("*Halter et al.*").

VII. ARGUMENTS

A. § 103(a) Rejection over *Akiyama et al.* and *Halter et al.*

The rejection of claims 1-5, 14-16, 18, 20-25, 29-34, and 38-41 under 35 U.S.C. § 103(a) as unpatentable over *Akiyama et al.* and *Halter et al.* is improper because *Akiyama et al.* and *Halter et al.* fail, either alone or in combination, to render obvious the content management method recited in claim 1 and the content management system recited in claim 20.

In the final Office Action and the Advisory Action mailed August 17, 2007 ("Advisory Action"), the Examiner fails to clearly articulate the pertinence of *Akiyama et al.* and *Halter et al.* to the claim elements. The key to supporting any rejection under 35 U.S.C. § 103 is the clear articulation of the reasons why the claimed invention would have been obvious. Such an analysis should be made explicit and cannot be premised upon mere conclusory statements. MPEP § 2142, 8th Ed., Rev. 6 (Sept. 2007) (emphasis added); see also *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, ___, 82 USPQ2d 1385, 1396 (2007). Moreover, "[w]hen a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained ..." 37 C.F.R. § 1.104(c)(2).

The Examiner fails to clearly articulate which elements taught by *Akiyama et al.* and *Halter et al.*, either alone or in combination, allegedly constitute "decrypting the encrypted content key using the first storage key" and "encrypting the decrypted content key using the second storage key," as recited in claim 1 (emphasis added). Thus, Appellants are only able to address the Examiner's rejection as it has been incompletely communicated in the final Office Action and the Advisory Action.

1. Claims 1-5, 14-16, and 18

Claims 1-5, 14-16, and 18 are not rendered obvious by *Akiyama et al.* and *Halter et al.* for at least the reason that *Akiyama et al.* and *Halter et al.* fail, alone or in combination, to render obvious all of the elements of the content management method recited in independent claim 1, from which claims 2-5, 14-16, and 18 depend. For example, combining the teachings of *Akiyama et al.* and *Halter et al.* in the manner that is suggested by the Examiner would result in an inoperable method.

Moreover, even assuming *arguendo* that the teachings of *Akiyama et al.* and *Halter et al.* were combined, there is still not any teaching or suggestion in the cited references of a content management method comprising, inter alia, "sending . . . the second storage key to a key management unit," as recited in claim 1. There is also not any teaching or suggestion in *Akiyama et al.* and *Halter et al.*, alone or in combination, of "decrypting the encrypted content key using the first storage key" and "encrypting the decrypted content key using the second storage key," as recited in claim 1.

Akiyama et al. discloses "a client authenticating system in a data distributing system having a data supplying apparatus for holding data and a client receiving the data via a communication interface from the data supplying apparatus" (col. 2, lines 46-

49). "The data supplying apparatus may be [] constructed to distribute [] encrypted data to the client. In this case, the client is constructed to include a first decrypting element for decrypting the encrypted data. The data supplying apparatus may be constructed to include a third encrypting element for encrypting [a] third key for decrypting the data by use of [a] first key. In this case, the client is constructed to include a second decrypting element for decrypting the encrypted third key by use of [a] second key. Then, the first decrypting element decrypts the encrypted data with the third key decrypted by the second decrypting element" (col. 3, lines 16-28). A "MASC [Media Access and Security Card] 5 is removably set in the service client 6" (col. 6, lines 26-27), and the MASC 5 has a "ROM 57 . . . for storing . . . [the] second key" (col. 10, lines 9-13).

Halter et al. discloses "a cryptographic means for protecting software distributed over an open channel or via a high-density stamped medium" (col. 5, lines 28-30). "When a customer purchases multimedia software from a software distribution facility, the customer provides his/her customer number. The customer key is produced from a set of variables consisting of an assigned customer number, a counter (arbitrarily set to zero), and a secret key-generating key (KGK) known only to the software distribution center. A special copy-right protected function (f) is then used to derive a variant customer key (KC') from the customer key. The data key(s) associated with the multimedia file(s) purchased by the customer are then encrypted with the variant customer key. The clear customer key and the encrypted file key(s) are provided to the customer . . . At the user processor, the keys and encrypted file(s) are initialized and made available to the file recovery program. The file recovery program decrypts and recovers the file(s)." (Col. 5, line 65 to col. 6, line 16.)

a. The combination of teachings from *Akiyama et al.* and *Halter et al.* that is suggested by the Examiner would result in an inoperable method.

It would not have been obvious to one of ordinary skill to combine the teachings of *Akiyama et al.* and *Halter et al.* to derive a content management method comprising, inter alia, "sending the encrypted content key and the second storage key to a key management unit," as suggested by the Examiner, for at least the reason that such a combination would result in an inoperable method or apparatus. There is no suggestion to modify a prior art device where the modification would render the device inoperable for its intended purpose. *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984); *In re Sponnoble*, 405 F.2d 578, 587, 160 USPQ 237, 244 (CCPA 1969).

The Examiner argues, "it would have been obvious . . . to modify the invention of Akiyama et al. by using the key distribution system disclosed by Halter, in order to prevent files from being decrypted except at appropriate user processors" (Final Office Action, page 3, paragraph 3). However, one of ordinary skill would understand that sending the "second key" of *Akiyama et al.* from the "client" to the "data supplying apparatus" of *Akiyama et al.* in an unencrypted form (i.e., as "plaintext") would expose the unencrypted "second key" to interception by a third party. By intercepting the unencrypted "second key," the encrypted data could be decrypted by the third party and the security intended by *Akiyama et al.* would therefore be compromised. Thus, since the system of *Akiyama et al.*, as modified by the Examiner, would be inoperable for its intended purpose, it would not have been obvious for one of ordinary skill to combine the teachings of *Akiyama et al.* and *Halter et al.* in the manner suggested by the Examiner.

b. *Akiyama et al.* and *Halter et al.* fail to teach or suggest, alone or in combination, "sending . . . the second storage key to a key management unit," as required by claim 1.

Moreover, even assuming *arguendo* that the teachings of *Akiyama et al.* and *Halter et al.* were combined, there is still not any teaching or suggestion in the cited references of "sending . . . the second storage key to a key management unit," as recited in claim 1 (emphasis added). Even the combination of *Akiyama et al.* and *Halter et al.* that is suggested by the Examiner fails to teach or suggest "sending . . . the second storage key to a key management unit," as required by claim 1.

The Examiner appears to rely on the "second key" of *Akiyama et al.* as allegedly constituting the "second storage key" recited in claim 1. However, *Akiyama et al.* is silent on the matter of "sending" this second key to any "key management unit," as required by claim 1 (emphasis added). For example, the MASC (5) of *Akiyama et al.* that stores the second key does not "send" the second key to any other "unit."

Halter et al. does not make up for the deficiencies of *Akiyama et al.* because *Halter et al.* is silent on the matter of "sending" the "second key" of *Akiyama et al.* "to a key management unit," as required by claim 1 (emphasis added). The Examiner does not rely on *Halter et al.* for any teaching or suggestion of this element of claim 1. The Examiner merely relies on *Halter et al.* for an alleged teaching of the "encrypted content key" recited in claim 1 (Final Office Action, paragraph bridging pages 7 and 8; emphasis added). Thus, *Halter et al.* also fails to teach or suggest "sending . . . the second storage key to a key management unit," as recited in claim 1.

c. *Akiyama et al.* and *Halter et al.* fail to teach or suggest, alone or in combination, "decrypting the encrypted content key using the first storage key" and "encrypting the decrypted content key using the second storage key," as required by claim 1.

In addition, it would not have been obvious for one of ordinary skill to obtain, from a combination of *Akiyama et al.* and *Halter et al.*, any teaching or suggestion of "decrypting the encrypted content key using the first storage key" and "encrypting the decrypted content key using the second storage key," as recited in claim 1 (emphasis added). Even the combination of teachings from *Akiyama et al.* and *Halter et al.* that is suggested by the Examiner fails to include "decrypting the encrypted content key using the first storage key" and "encrypting the decrypted content key using the second storage key," as recited in claim 1.

The Examiner provides a vague indication of where the "content key," "first storage key," and "second storage key" allegedly read on isolated elements of *Akiyama et al.* and *Halter et al.* (Final Office Action, page 8, paragraph 4 to page 9, paragraph 3). However, claim 1 recites the content key, first storage key, and second storage key, not in isolation, but rather within limitations that interrelate these elements, such as "decrypting the encrypted content key using the first storage key" and "encrypting the decrypted content key using the second storage key" (emphasis added). The Examiner's rejection fails to address these claimed relationships in regard to *Akiyama et al.* or *Halter et al.* Indeed, *Akiyama et al.* and *Halter et al.* are silent on the matter of "decrypting the encrypted content key using the first storage key" and "encrypting the decrypted content key using the second storage key," as recited in claim 1 (emphasis added).

Thus, the Examiner's proposed combination of *Akiyama et al.* and *Halter et al.* fails to teach or suggest all of the elements recited in claim 1. Furthermore, the Examiner has not identified any reason why one of ordinary skill would otherwise modify *Akiyama et al.* and *Halter et al.*, either alone or in combination, to obtain all of the elements recited in claim 1. Since *Akiyama et al.* and *Halter et al.* do not render obvious the content management method recited in claim 1, claim 1 and claims 2-5, 14-16, and 18, which depend therefrom, are allowable over *Akiyama et al.* and *Halter et al.* and this rejection should be withdrawn.

2. Claims 20-25, 29-34, and 38-41

Claims 20-25, 29-34, and 38-41 are not rendered obvious by *Akiyama et al.* and *Halter et al.* for at least the reason that *Akiyama et al.* and *Halter et al.* fail, alone or in combination, to render obvious all of the elements of the content management system recited in independent claim 20, from which claims 21-25, 29-34, and 38-41 depend. For example, combining the teachings of *Akiyama et al.* and *Halter et al.* in the manner that is suggested by the Examiner would result in an inoperable system.

Moreover, even assuming *arguendo* that the teachings of *Akiyama et al.* and *Halter et al.* were combined, there is still not any teaching or suggestion in the cited references of a content management system comprising, inter alia, "a sending means for sending . . . the second storage key to a key management unit," as recited in claim 20. There is also not any teaching or suggestion in *Akiyama et al.* and *Halter et al.*, alone or in combination, of "a first decrypting means . . . for decrypting the encrypted content key using the first storage key" and "an encrypting means for encrypting the decrypted content key using the second storage key," as recited in claim 20.

a. The combination of teachings from *Akiyama et al.* and *Halter et al.* that is suggested by the Examiner would result in an inoperable system.

As already discussed, it would not have been obvious to one of ordinary skill to combine *Akiyama et al.* and *Halter et al.* to derive "sending the encrypted content key and the second storage key to a key management unit," as suggested by the Examiner, for at least the reason that such a combination would result in an inoperable method or apparatus.

b. *Akiyama et al.* and *Halter et al.* fail to teach or suggest, alone or in combination, "sending . . . the second storage key to a key management unit," as required by claim 20.

Moreover, even assuming *arguendo* that the teachings of *Akiyama et al.* and *Halter et al.* were combined, there is still not any teaching or suggestion in the cited references of "a sending means for sending . . . the second storage key to a key management unit," as recited in claim 20 (emphasis added). Even the combination of *Akiyama et al.* and *Halter et al.* that is suggested by the Examiner fails to teach or suggest "sending . . . the second storage key to a key management unit," as required by claim 20.

Akiyama et al. is silent on the matter of "sending" this second key "to a key management unit," as required by claim 20 (emphasis added). For example, the MASC (5) of *Akiyama et al.* that stores the second key does not "send" the second key to any other "unit." *Halter et al.* does not make up for the deficiencies of *Akiyama et al.* because *Halter et al.* is silent on the matter of "sending" the "second key" of *Akiyama et al.* "to a key management unit," as required by claim 20 (emphasis added).

c. *Akiyama et al.* and *Halter et al.* fail to teach or suggest, alone or in combination, "decrypting the encrypted content key using the first storage key" and "encrypting the decrypted content key using the second storage key," as required by claim 20.

In addition, it would not have been obvious for one of ordinary skill to obtain, from a combination of *Akiyama et al.* and *Halter et al.*, any teaching or suggestion of "a first decrypting means . . . for decrypting the encrypted content key using the first storage key" and "an encrypting means for encrypting the decrypted content key using the second storage key," as recited in claim 20 (emphasis added). Even the combination of teachings from *Akiyama et al.* and *Halter et al.* that is suggested by the Examiner fails to include "decrypting the encrypted content key using the first storage key" and "encrypting the decrypted content key using the second storage key," as recited in claim 20.

The Examiner's rejection fails to point out where these claim limitations can allegedly be found in *Akiyama et al.* or *Halter et al.* Indeed, *Akiyama et al.* and *Halter et al.* are silent on the matter of "decrypting the encrypted content key using the first storage key" and "encrypting the decrypted content key using the second storage key," as recited in claim 20 (emphasis added).

Thus, the Examiner's proposed combination of *Akiyama et al.* and *Halter et al.* fails to teach or suggest all of the elements recited in claim 20. Furthermore, the Examiner has not identified any reason why one of ordinary skill would otherwise modify *Akiyama et al.* and *Halter et al.*, either alone or in combination, to obtain all of the elements recited in claim 20. Since *Akiyama et al.* and *Halter et al.* do not render obvious the content management system recited in claim 20, claim 20 and claims 21-

25, 29-34, and 38-41, which depend therefrom, are allowable over *Akiyama et al.* and *Halter et al.* and this rejection should be withdrawn.

B. CONCLUSION

For the reasons given above, pending claims 1-5, 14-16, 18, 20-25, 29-34, and 38-41 are allowable and reversal of the Examiner's rejection is respectfully requested.

To the extent any extension of time under 37 C.F.R. § 1.136 is required to obtain entry of this Appeal Brief, such extension is hereby respectfully requested. If there are any fees due under 37 C.F.R. §§ 1.16 or 1.17 that are not enclosed herewith, including any fees required for an extension of time under 37 C.F.R. § 1.136, please charge such fees to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 3, 2007

By:____________________
Reece Nienstadt
Reg. No. 52,072

VIII. CLAIMS APPENDIX TO APPEAL BRIEF UNDER RULE 41.37(C)(1)(VIII)

1. A content management method for managing content data provided to user equipment, comprising the steps of:

storing a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key in the user equipment;

sending the encrypted content key and the second storage key to a key management unit;

at the key management unit, decrypting the encrypted content key using the first storage key, the first storage key being stored in the key management unit;

encrypting the decrypted content key using the second storage key;

sending the content key encrypted with the second storage key to the user equipment; and

at the user equipment, decrypting the encrypted content key using the second storage key and decrypting the content data using the decrypted content key.

2. The method as set forth in Claim 1, wherein the second storage key is generated based on a random number.

3. The method as set forth in Claim 1, wherein the decrypted content key is encrypted with identification information of the user equipment and stored into the user equipment.

4. The method as set forth in Claim 1, wherein the content key is encrypted, in the user equipment, with the first storage key and identification information of the user equipment, and the content key stored in the user equipment is decrypted with the first storage key and the identification information of the user equipment.

5. The method as set forth in Claim 1, wherein the second storage key is generated by a decrypted key generating means provided in the user equipment.

6. The method as set forth in Claim 5, wherein the second storage key is encrypted with a public key for the key management unit for management of the storage keys to generate a third storage key and the third storage key is stored into the user equipment.

7. The method as set forth in Claim 6, wherein the user equipment deletes the second storage key depending upon whether the third storage key has been stored in the user equipment.

8. The method as set forth in Claim 7, wherein, when decrypting the content key stored in the user equipment, the user equipment sends the third storage key to the key management unit; and the key management unit generates the second storage key based on the third storage key while performing an accounting following a predetermined procedure.

9. The method as set forth in Claim 1, wherein the second storage key is generated by a storage key generating means provided in the key management unit which manages the storage keys; and the key management unit has stored therein the second storage key and identification information of the user equipment in which the content key encrypted with the above generated second storage key is stored.

10. The method as set forth in Claim 9, wherein upon the generation of the second storage key, the key management unit performs an accounting following a predetermined procedure.

11. The method as set forth in Claim 9, wherein the key management unit encrypts the second storage key with the management key to generate a third storage key, and sends the third storage key to the user equipment; and the user equipment stores the received third storage key.

12. The method as set forth in Claim 11, wherein the user equipment deletes the second storage key depending upon whether the third storage key has been stored.

13. The method as set forth in Claim 12, wherein the key management unit has stored therein the identification information of the user equipment in which the content key encrypted with the second storage key is stored; the user equipment sends, when decrypting the content key stored in the user equipment, the identification information of the user equipment to the key management unit; and the key management unit generates the second storage key based on the result of comparison between identification information of the user equipment, sent from the user equipment, and the identification information of the user equipment, held in the key management unit itself, while accounting the data service following the predetermined procedure.

14. The method as set forth in Claim 1, wherein the user equipment has stored therein identification information of the user equipment.

15. The method as set forth in Claim 14, wherein the user equipment starts decrypting the content key stored in the user equipment depending upon the result of an inspection of the identification information of the user equipment, stored in the user equipment.

16. The method as set forth in Claim 1, wherein the decrypted content key supplied from the user equipment has added thereto information that the content key has been obtained by restoration.

17. The method as set forth in Claim 16, wherein when moving the content key having added thereto the information that the content key has been obtained by restoration, the user equipment performs an error process based on the result of comparison between the content key and another content key stored in a destination to which the content key is to be moved.

18. The method as set forth in Claim 1, wherein the content key has added thereto frequency information that limits the number of times the content key can be used.

19. The method as set forth in Claim 1, further comprising storing the content key encrypted with the second storage key in a first storage of the user equipment along with identification information of the first storage; storing the content key that is stored in the first storage, and the identification information of the first storage, into a second storage of the user equipment; and performing, when a request is made to decrypt the content key in the first storage, an error process based on the result of comparison between the identification information of the first storage and the identification information of the second storage.

20. A content management system for managing content data, comprising:

a storing means having stored therein a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key;

a sending means for sending the encrypted content key and the second storage key to a key management unit;

a first decrypting means, in the key management unit, for decrypting the encrypted content key using the first storage key, the first storage key being stored in the key management unit;

an encrypting means for encrypting the decrypted content key using the second storage key; and

a second decrypting means for decrypting the encrypted content key using the second storage key and decrypting the content data using the decrypted content key.

21. The system as set forth in Claim 20, further comprising storage key generating means for generating the second storage key by means of a random number generator.

22. The system as set forth in Claim 20, wherein the encrypting means encrypts the decrypted content key with identification information of the storing means.

23. The system as set forth in Claim 20, wherein the content key is encrypted, in the storing means, with the first storage key and identification information of the storing means; and the content key stored in the storing means is decrypted with the first storage key and the identification information of the storing means.

24. The system as set forth in Claim 20, wherein the storing means, first decrypting means, and encrypting means form together a data storage, and wherein the key management unit manages the second storage key of the data storage.

25. The system as set forth in Claim 24, wherein the data storage is a data receiver that receives a content data encrypted and sent from a data transmitter.

26. The system as set forth in Claim 24, further comprising means for storing a public key of the key management unit; and wherein the storing means has stored therein the second storage key along with a third storage key obtained by encrypting the second storage key with the public key.

27. The system as set forth in Claim 26, wherein the data storage deletes the second storage key depending upon whether the third storage key is stored in the storing means.

28. The system as set forth in Claim 27, wherein, when decrypting the content key stored in the storing means, the data storage sends the third storage key to the key management unit; and the key management unit sends the second storage key generated based on the third storage key to a data transmitter while performing an accounting following a predetermined procedure.

29. The system as set forth in Claim 24, wherein the storing means has stored therein identification information of the data storage.

30. The system as set forth in Claim 29, wherein the data storage starts decrypting the content key stored in the storing means depending on the result of inspection of the identification information of the data storage, stored in the storing means.

31. The system as set forth in Claim 20, wherein the storing means, first decrypting means, and encrypting means form together a data storage; and further comprising a storage key generating means, wherein the key management unit manages the second storage key of the data storage.

32. The system as set forth in Claim 31, wherein the data storage is a data receiver that receives a content data encrypted and sent from a data transmitter.

33. The system as set forth in Claim 31, wherein the key management unit comprises an identification information storing means in which identification information of the storing means is stored.

34. The system as set forth in Claim 31, wherein the key management unit performs an accounting following a predetermined procedure depending upon a generation of the second storage key.

35. The system as set forth in Claim 31, wherein the key management unit comprises means for storing storage keys; the key management unit generates a third storage key by encrypting the second storage key with a management key and sends the third storage key to the data storage; and the data storage stores the third storage key into the storing means.

36. The system as set forth in Claim 35, wherein the data storage deletes the second storage key depending upon whether the third storage key is stored in the storing means.

37. The system as set forth in Claim 36, wherein the key management unit comprises means for storing the second storage key and identification information of the storing means in which the content key encrypted with the second storage key is stored; the key management unit performs an accounting, when the data storage decrypts the content key, following a predetermined procedure based on the result of comparison between the identification information of the storing means, sent from the data storage, and identification information stored in an identification information storing means.

38. The system as set forth in Claim 31, wherein the storing means has stored therein identification information of the data storage.

39. The system as set forth in Claim 38, wherein the data storage starts decrypting the content key stored in the storing means.

40. The system as set forth in Claim 20, wherein the content key obtained by decryption from the storing means has added thereto information that the content key has been obtained by restoration, as requirement information.

41. The system as set forth in Claim 20, wherein the content key has added thereto frequency information that limits the number of times the content key can be used.

IX. EVIDENCE APPENDIX TO APPEAL BRIEF UNDER RULE 41.37(C)(1)(IX)

Appellants do not rely, in the pending appeal, upon any evidence referred to in 37 C.F.R. § 41.37(c)(1)(ix).

X. RELATED PROCEEDINGS APPENDIX TO APPEAL BRIEF UNDER RULE 41.37(C)(1)(X)

There are currently no other proceedings, of which Appellants, Appellants' legal representative, or Assignee are aware, that will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.